PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-336169**
(43)Date of publication of application : **18.12.1998**

(51)Int.Cl. **H04L 9/32**

(21)Application number : **09-138724**
(22)Date of filing : **28.05.1997**

(71)Applicant : **NIPPON YUNISHISU KK**
(72)Inventor : **YATSUKAWA NAONOBU**

(54) **AUTHENTICATING METHODAUTHENTICATING DEVICESTORAGE MEDIUMAUTHENTICATING SERVER AND AUTHENTICATING TERMINAL**

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authenticating method which prevents a third person from reusing stolen authentication information.
SOLUTION: A server preserves a 1st check data (value = Dn-1) which checks authentication information of a clientand the client also preserves a 1st seed data (value = Dn-1) which generates authentication information. The client enciphers an authentication information request that is sent from the server by using his security key Ks and generates authentication information (value = Dn) and answers by sending it to the server. The server performs decoding through the public key Kp of the clientgenerates 2nd check data (value = Dn-1) and compares it with the 1st check data (value = Dn-1). When they coincidethe server allows the authentication request and preserves authentication information Dn in exchange for the 1st check data. When the client receives permissionhe preserves authentication information (value = Dn) as a 2nd seed data in exchange for the 1st seed data (value = Dn-1).

CLAIMS

[Claim(s)]
[Claim 1]A way characterized by comprising the following an authentication person attests an authentication demand person with a public-key crypto system to a demand of attestation from an authentication demand person.
A preservation process of saving the 1st examination report for an authentication person to inspect an authentication demand person's certification information beforehand.
An authentication demand sending-out process that said authentication demand person sends an authentication demand to said authentication person.
Said authentication person is a **** certification information demand process by sending a certification information demand to said authentication person to an authentication demand sent by said authentication demand person.
In order for said authentication demand person to answer said certification information

demand and to generate certification informationwhile said authentication demand person sends the 1st certification information that enciphered and generated the 1st species information that self holds using said authentication demand person's secret key to said authentication personA certification information sending-out process of changing said 1st generated certification information to said 1st species information currently held as the 2nd species information for a next authentication demandand saving itand said authentication personBy decrypting said 1st certification information sent by said authentication demand person by said authentication demand person's public keyGenerate the 2nd examination report and a comparison process in comparison with forward [said]with said 1st saved examination report and said authentication person this 2nd examination reportAn updating process of notifying said authentication demand person of permitting said authentication demand when said 2nd examination report is in agreement with said 1st examination reportand replacing with said 1st examination report and saving said 2nd examination report.

[Claim 2]An authentication server which saves certification information for giving attestation to an authentication demand from two or more authentication demand personscomprising:
A means to memorize an examination report for inspecting an authentication demand person's certification information for every authentication demand person.
A means to send a certification information request message to the authentication person if an authentication demand from arbitrary authentication demand persons is receivedCertification information sent by the authentication demand person is decrypted by the authentication demand person's public keyWhen an examination report is newly generated and a means [forward / said /with a saved examination report / examination report / this / that was newly generated] and said newly generated examination report are in agreement with said saved examination reportpermit said authentication demandand. A means to replace with said saved examination report and to save said newly generated examination report.

[Claim 3]An authentication device which gives attestation to an authentication demand from an authentication demand person with support of an external authentication servercomprising:
A memory measure which memorizes species information for generating certification information which attests said authentication demand person.
A transmission and reception means which an authentication demand message is sent to said authentication serverand receives a certification information request message from said authentication server which answers this authentication demand message.
An encoding means which generates certification information to a certification information request message from said authentication server by enciphering said species information memorized to said memory measure using a secret key.
An attestation delivery means which generated certification information is sent to said authentication serverand changes to said species information memorized in said memory measureand memorizes this generated certification information.

[Claim 4]An authentication terminal device which gives attestation to an authentication

demand through a storage from an authentication demand person supported by an external authentication servercomprising:
A main part.
Have an interfacing means for receiving a storage which memorizes a program which generates certification information using said secret key from species information for generating certification information which attests an authentication demand persona secret key about the authentication demand personand said species informationand said main partA reception means which receives an authentication demand from said authentication demand person.
A request means which answer this authentication demandand an authentication demand message is sent to said authentication serverand receives a certification information request message from said authentication server which answers this authentication demand.
Answer a certification information request message and via said interfacing meansAre a commanding means which performs a program in said storageand said program is receivedreturn certification information which was made to generate this authentication demand person's certification information using said secret keyand was generated from said species information to said main part via said interfacing means -- it closing and. A commanding means which makes said species information in said storage update by this generated certification informationand a certification information delivery means which sends returned certification information to said authentication server.

[Claim 5]A storage which memorizes an authentication program which gives attestation to an authentication demand from an authentication demand person with support of an external authentication servercomprising:
The 1st program code that makes a predetermined memory measure memorize species information for said authentication program to generate certification information which attests said authentication demand person.
The 2nd program code that sends an authentication demand message to said authentication server.
The 3rd program code that receives an authentication demand message from said authentication server.
Send the 4th program code that generates certification information using a secret key from said species information memorized to said memory measureand generated certification information to said authentication server to a certification information request messageand. The 5th program code that changes to said old species information and memorizes this generated certification information as new species information.

[Claim 6]The authentication method according to claim 1 characterized by not performing replacement preservation when said certification information sending-out process replaced and saves said 1st species information by said 2nd species information when a notice of a purport which permits an authentication demand is receivedand a notice is not received.
[Claim 7]The authentication device according to claim 3 when said attestation delivery means updates said species information when a notice of a purport which permits an authentication demand is received from said authentication serverand a notice is not

receivedwherein it does not update.
[Claim 8]The authentication terminal device according to claim 4 with which said commanding means is characterized by making said species information update when a notice of a purport which permits an authentication demand to a program in said storage is received from said authentication serverand not making it update when a notice is not received.
[Claim 9]When a notice of a purport which permits an authentication demand to a program in said storage is received from said authentication serversaid 5th program codeThe storage according to claim 5 by which the 6th program code that does not update being included when said species information is updated and a notice is not received.
[Claim 10]The authentication method according to claim 1 using said authentication demand person's identification information as an initial value of said 1st species information.
[Claim 11]The authentication device according to claim 3 using said authentication demand person's identification information as an initial value of said species information.
[Claim 12]The authentication terminal device according to claim 4 using said authentication demand person's identification information as an initial value of said species information.
[Claim 13]The authentication method according to claim 1 characterized by sending certification information to said authentication person with a public key certification in said certification information sending-out process.
[Claim 14]The authentication device according to claim 3wherein said certification information delivery means sends certification information to said authentication server with a public key certification.
[Claim 15]The authentication terminal device according to claim 4wherein said certification information delivery means sends certification information to said authentication server with a public key certification.
[Claim 16]The authentication server according to claim 2wherein said memory measure memorizes a public key for every authentication demand person with an examination report.
[Claim 17]The authentication method according to claim 13wherein an authentication person saves a sent public key certification.
[Claim 18]The authentication method according to claim 1 refusing said authentication demand by said authentication demand person when said 1st examination report is not in agreement with said 2nd examination report.
[Claim 19]The authentication server according to claim 2 refusing said authentication demand by said authentication demand person when said newly generated examination report is not in agreement with said saved examination report.
[Claim 20]The authentication method according to claim 1 enciphering as only a genuine owner can decrypt said authentication demand person's secret key.
[Claim 21]The authentication terminal device according to claim 4wherein said storage is an IC card.
[Claim 22]The authentication terminal device according to claim 4 which said storage memorizes a password further and compares further a password entered by said authentication demand person with a password memorized by said storageand is

characterized by said storage returning certification information to said main part only when in agreement.
[Claim 23]The authentication terminal device according to claim 4wherein conversion to certification information from species information using a secret key was performed only in a storageand said secret key was not sent to said main part side and made.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the authentication server as the storage which memorized the program for the authentication method of the other party who passed the networkfor examplean authentication deviceand an authentication deviceand an authentication person who participates in the attestation.
[0002]
[Description of the Prior Art]The security protection to the information and telecommunications between the individuals through a networkbetween individual 1 companiesor between companies has been a pressing technical problem now when an information processing system came to play a central role in all the aspects of affairs of a social activity. The security function is indispensable to a field like extra-sensitive-information transmission or electronic commerce technology (Electronic Commerce) by open-izing and wide use of the network system of these days especially. For examplewhen a juristic act is made between companiesbetween individualsor by these mutualsWhen draw up a contract etc.sign conventionally using physical paper (now)and a seal is sealedand also the notarial deed by the seal registration card or a notary public is attached if needed and then these documents are sent to the other partyregistered mail is used or it is made a content-certified mail.
[0003]It is the network security art which closes all the acts centering on such physical documents by electronic information and telecommunications if it is substitution safely. Such [now] a demand to which the information-and-telecommunications network by the computer and a network reached the whole-world scale is a way of increase. The purpose of network security is in network securityand it is supposed that it is it protecting the information according to the degree of secrecy of the network system from various threats. Generallyit is defined as maintaining ** confidentiality (Confidentiality)** completeness (Integrity)** availability (Availability)and ** denial refusal (Non-Repudiation). On the other handas a typical threat assumed to a networkthey are tappingdisclosurespoofingan alteration/forgeryan unauthorized entry/unlawful accessusurpationfactual denialdestructionetc.
[0004]There are secrecy / preservation artauthentication technologykey delivery artdenial refusal artthird party financial institutionan access controlsecurity audita security valuation basisetc. as a component engineering of a network security sake. When performing the information and telecommunications through a network systemchecking who has used the system howor controlling and managing maintains securityit is importantand indispensable. The most event which happens within a system should originate in the specific substance (entity) in connection with information and

telecommunicationstherefore it can be said that those recognition is the foundations of security reservation.
[0005]It is thought that attestation is checking whether the substance (entity: a processsoftwarehardwarecommo dataetc. which function as a substitute of human being and human being) which participated in information and telecommunications being just. Generallyas shown in Drawing 1it can classify according to the substance to attest. Entity attestation is checking justificationsuch as transmission and reception of the substance in connection with information and telecommunicationsfor examplea messageandon the other handit can be said that message attestation is checking the justification of these sent received messages. Entity attestation may be called user authentication.
[0006]An entity authentication device is divided into entity identification processing and entity authenticating processing. The former identifies who the user of a system is and the latter is processing in which the user checks whether you are the just person himself/herself. Although a user identifier (User-id) etc. are generally used for the formerthis is a publicly known identifier and the original authenticating processing using the informationincluding a passworda passwordetc.which only the person himself/herself has is left to the latter processing.
[0007]The following entity authentication devices have described this entity authenticating processing. It is large and can classify into fourknowledge usecode usepossessions useand the living body feature useaccording to the state of information used for attestation at an entity authentication device. These are explained in order.
[0008]<Knowledge use> The entity attestation by knowledge use registers information required in order to attest an entity beforehandand is the method of checking the justification of the entity by whether the entity which should be attested knowing the information. A "password"a "password"or "the informationincluding an addressa date of birthetc.which cannot be known only to the individual" are best used by personal authentication etc.
[0009]In most systemsthe "password" is performing user authentication. Although the entity attestation by such knowledge use is comparatively easy to introduce and it is effectiveits danger of using the character string which is easy to memorizeor making a note at the place which is easily conspicuousand it being easily detected by othersor being intercepted during communication is high. If it is the password same each time even if it enciphers at the time of password transmissionspoofingis possible by using it by stealth as it isand reusing it (replay attack). The password file (it was enciphered as a key and the user's password is usually saved) by the side of a server may be broken by a dictionary attack.
[0010]In order to oppose these threatsthe device of changing a password each time is needed. Thereforein entity attestation of knowledge usethe password method only for [such as a one-time password method and a challenge response method / whichon the other handused the tropism function and the random number / advanced] 1 time is devisedfor example. Each method is described below.
(1) As the one-time password method characterit is advocated once by BellcoreCo.U.S.A by the pass-word-authentication method of a limitationand is RFC-ized also as an Internet standard (RFC-1938). Belowthe processing outline of the most famous S/Key method is explained.
[0011]A S/Key method is 1when A is made into a client and it makes B an authentication

server. : On the other handthe tropism random number f is prepared.
2: A generates the arbitrary numerical values S called the secret random number R and an open kind.
3: Consider it as Q=R+S and they are f (Q)f (f (Q))and f (f (f (Q)))-- is calculated and they are made into $X_1X_2X_3$--$X_{100}$and X_{101}.
[0012]4: A holds secretly X_1--$X_{100}$and Rand pass X_{101} to B by a certain method (off-line)and B holds them.
5: When A logs in to B for the first timetransmit X_{100} to B as a password.
6: B calculates f (X_{100}) and compares it with X_{101} currently held. If in agreementlogin is permittedand login will be refused if not in agreement. When login is permittedB throws away X_{101} and holds X_{100}.
[0013]7: When A logs in to the nextuse password X_{99} of the following. Processing after the B side is performed similarly.
Since it is a password only for - 1 time as a strong point of a S/Key methodit is not recyclable even if a third party intercepts on the way of [communication].
[0014]- The password currently held on the file of the server B is for inspecting the password at the time of login next time.
It is convenient even if this is stolen.

- Since the function f is a tropism function on the other handeven if X_n is interceptedX$_{n-1}$ is incalculable. Thereforeit is convenient even if f is known by the third party.
Howeveras demerit of a S/Key methodif a 100-piece password is exhaustedthe time and effort which carries out reinitialization of the authentication program of a server is required of the case on -.
[0015]- It is always necessary to hold the random number R in the server side so that it may be on line possible in the above-mentioned reinitialization in a actual system. That isat the time of reinitializationa client transmits only different seed S' from before to a server on-line (even if S' is interceptedit is satisfactory)and a server newly calculates Q'=R+S' using R currently heldand generates X'$_{101}$ new from now on. For this reasonif a third party invades into a server by a certain method or a server manager gets this random number with malicious intenta password is generableand it becomes the client A and can clear up.
(2) a challenge response method -- this is a kind of the measure against tapping in pass word authenticationand a CHAP (Challenge Authentication ProtocolRFC-1334) method is typical. In this CHAP methodthe procedure the authentication demand person A gets the authentication person B to attest is as in Drawing 2.
[0016]Since the password of A is held on B while there is the strong point in which a third party intercepts the message of ** in a figureand potato reuse is impossiblesince a challenge changes each timea challenge response methodThe administrator of B itself abuses it and is having the demerit in which it can become the client Ait can clear up and injustice can be performed pointed out.
[0017]<Code use> Using a code for entity attestation is a technique which generates certification information with difficult forgeryand checks the justification of the party concerned (entity) using encoding technology in addition to the party concerned when the parties concerned exchange and inspect it.
(1) It is considered to be requirements a digital signature digital signature is a mechanism

in which personal identification with the signature and seal in the conventional document dealings is performed on electronic mediaand fulfill the following three conditions functionally.
[0018]
** A signature sentence cannot forge by a third party.
** A signature sentence cannot forge by an addressee.
** A sending person cannot deny later the fact of having sent the contents of the signature sentenceand it.
In order to satisfy the requirements for ** and ** under the present circumstancesuse of a public-key crypto system is indispensable. A public key crypto system is the concept announced by Diffie (Diffie) of Stanford Universityand Hermann (Hellman) in 1976the enciphering key and decryption key of a couple may differ from each otheronly a decryption key may be held secretlyand an enciphering key may be exhibited. Thereforeit is said that it has the featuressuch as that delivery of a key is easythat there are few kinds of key held secretly and they endand having an authentication function (digital signature). The common model of a public-key crypto system is shown in Drawing 3.
[0019]If relation between this public key and a secret key is made reverseit will become a digital signature function. That isa plaintext is enciphered with the secret key which only a sending person gets to knowand it transmits to an addressee. An addressee decrypts by a sending person's public keyand gets a plaintext. In this casesince only a sending person knows an enciphering keya cryptogram can forge by the third party and an addressee. Since the contents of the plaintext can be enciphered only to the person himself/herself with an enciphering key and it cannot transmit to hima sending person cannot deny the fact of having become behind and having sent the contents of the cryptogramand itbut the requirements for an above-mentioned digital signature are satisfied.
[0020]Nowas most leading algorithm in the world where the concept of this public key encryption was realizedit is developed by RivestShamirand Adleman of MITand there is RSA cryptograph which took each initial and was named. There are the following two as a digital signature system currently standardized internationally.
- Attestation child checking method (with appendix) -- ISO/IEC CD 14888 PART1/2 / 3 (Sep 21-1995)and the correspondence restoring method (giving message recovery) -- ISO/IEC. 9796:1991 (E) The former attestation child checking method is actually used widelyand the outline is shown in Drawing 4.
[0021]In order for an addressee to verify a sending person's justification using a digital signaturethe guarantee which belongs to the sender of truth [public key / of a sending person] is required. For examplethe thing equivalent to the seal registration card proving a physical seal being just is needed for a digital signature. The public key certification system by the third party who can trust it for this guarantee is providedand that issuing agency is called CA (Certification Authority). CA is enacted as an Internet standard (RFC1421-1424)and performs issue and management of a public key certification.
[0022]The format of the certificate is enacted as international standards (X.509 ->ISO9594-8).
The third edition has come out of X.509and the ISO standard corresponding to it is also already due to be enacted from now on.
A certificate consists of itemssuch as a user's identifiera user's public keythe term of validity of a certificatea serial numberan issuing agency nameand a digital signature of an

issuing agencyand the electronic signature of the CA concerned is attached after these.
[0023]In the example of Drawing 4the sending person A transmits the public key certification of this A to B with the digital signature of A given to the transmitting text and it. By inspecting the digital signature by CA of this public key certification firstthe addressee B checks the justification of the public key certification of A. If this was justB is able to obtain the public key of just A. ThenB performs sending person attestation by inspecting the digital signature of A.
[0024]If strict CA exists as a strong point of an attestation child checking method and a sending person can hold an own secret key strictlythe point that "spoofing" by a third party is generally difficult is pointed out. Howeverin the remote login through a networkwhen a signature is used as a password for remote login (that isa digital signature is used as partner certification information). The demerit of being possible also has "spoofing" by what (replay attack) a third party intercepts it and reuses as it is.
(2) an authentication token method with a digital signature -- this can be said to be having improved the intensity to the replay attack of the method of (1). The outline of processing of an authentication token method with a digital signature is shown in Drawing 5.
[0025]Namelyas a premise of this methodas for the client Athe server B presupposes the public key certification of A by which the digital signature was carried out with the secret key of CA again that the public key of CA is held. In this statethe client A transmits to the server B what was assembled from ** to ** of the following as certification information (an authentication token is called hereafter). The time stamp T at the time of token creation is contained in this authentication token.
[0026]
** : the public key certification of A (Ca)
** : time stamp (T)
** : the digital signature of **;**+**such as an E-Mail address of addressee id:B (Sa)
The server B which received this authentication token inspects a signature firstand after checking that the time stamp T etc. are not alteredthis T and current time are compared. If a comparison result is almost equallogin of the client A will be permitted.
[0027]Howeverif T is the past time beyond in fixed timethis authentication token will regard it as what is reused by third parties other than A and B (replay attack)and will refuse login. If strict CA exists and a sending person can hold an own secret key strictlythis token methodIf it is in fixed time while "spoofing" by a third party has the strong point of being quite difficultspoofingalso has the demerit of being possibleby reusing the intercepted authentication token as it is (replay attack).
(3) SSH (Secure SHell) method SSH methods are security packages to as opposed to a command process r systemsuch as rsh/rlogin for the remote login in UNIXand are examined as an Internet draft. Although the portion about authenticating processing is shown belowit is the challenge-response authentication method which used together a common key encryptosystem and public key encryption fundamentally.
[0028]Drawing 6 is a sequence at the time of the client A logging in to the server B. in the figure -- common key encryptosystems (DESIDEAetc.) -- it is divided into the phase (****) for sharing the session key of businessand the phase (******) which performs authenticating processing. The processing sequence is as follows.
** The client A sends a login request to the server B.
[0029]** Based on this login requestthe server B sends an own public keya random

numberetc. to the client A for a session key share.
** The client A generates a session keyenciphers it by the public key of the server Band sends it to B. Since a session key is able to be shared to the client A and during this period when the server B receives thisafter **with this session keyit enciphers and all the messages between AB(s) are carried out.
[0030]** The client A sends an own public key and a user name to the server B.
** After checking that the public key and user name of the client A are registeredthe server B generates the challenge (random number) for attestationenciphers it by the public key of Aand it sends it to the client A.
** The client A calculates the hash value of the above-mentioned challengeand sends it to the server B by making it into a challenge response.
[0031]** the server B was saved with the value of the challenge response received by ** -- it client A turns and the hash value of a challenge is comparedand if it is equivalentlogin of A is permittedand login will be refused if it differs. Since challenge data change each timeeven if a third party intercepts the message of **it is said the strong point of a SSH method "cannot be become completely" completely according to reusebut. As demeritwhen the administrator of the - server B itself rewrites the public key information on the client A with malicious intentit is pointed out that it is possible to become the client Ato clear up and to perform injustice.
(4) The PRC (Remote Procedure Call) authentic method of PRC ********** is a remote procedure call function in which it is well used by a UNIX distributed-environment system.
The user authentication function is prepared as a security function.

[0032]It has the function in which a server checks who the publisher of RPC procedure of this RPC attestation isand how much that publisher's authority is (entity authentication function). The outline of the entity authentication function which this PRC attestation has describes the outline of that procedure so that it may be Drawing 7.
** In advance of communicationa client and a server share first the common key (K_{ab}) used for a DES code by a DH process (the Diffie-Hellman type public key delivering method). In the UNIX worldthe public key and secret key which are used for a DH processEach user obtains the public key of a communications partner and the own secret key which have been beforehand registered from this NIS in advance of communication by being managed by NIS (Network Infomation Service)and a common key (DES key) is obtained by calculation.
[0033]** In a clientcreate certification information in the following procedure and transmit to a server. (I) Generate the character string (called a net name) showing a sending person. In the case of UNIXit has the form unix.< user id>@ <host address>.
[0034](II) Generate a session key (random number: K).
(III) Carry out DES encryption of the time stamp (current time: T) with a session key (K) (Te).
(IV) Carry out DES encryption of the session key (K) with a common key (K_{ab}) (K_e). The net name of (I)the time stamp (T_e) in which (III) was enciphered the session key (K_e) of (IV)etc. are transmitted to a server as certification information.
[0035]** A server verifies the justification of a net name by decrypting the enciphered time stamp (T_e) in the received certification informationand comparing (T) and it with

current time. That isif the difference of T and current time is in tolerance levelthe access request of the net name will be permittedbut if it is outside tolerance levelit will refuse. If each of a client and a server can hold an own secret key strictly and a just partner's public key can be certainly obtained as a strong point of a RPC authentic methodspoofingby the 3rd person is generally said to be difficultbut. If it is in fixed timespoofingalso has the demerit of being possibleby reusing the intercepted certification information as it is (replay attack).
(5) Kerberos (RFC1510) method Kerberos is the user authentication system developed in the Athena project of MIT.
It is based on the "authentic method by the trusted third party period" proposed by R.Needham and M.Schroeder in 1978.
This Kerberos was adopted as authentication service in DCE (Distributed Computing Environment) which is a software package for the distributed-processing-environment construction which OSF (Open Software Foundation) defined.
[0036]In this methodonly the common key encryption system (DES) has realized communicative secrecyuser authenticationetc. altogether. Knowing each user's key has adopted the method of having mutual justification guaranteed by an authentication server on the assumption that it is only each user itself and an authentication server.
[0037]It is devising so that the portion which hits an authentication server may be divided into a Kerberos server and TGS (Ticket Granting Server: ticket issue server) and a user's password or key may not be held for a long time on the system (a security level is low) by the side of a user. The idea of ticket (Ticket) and OSEN Decatur (Authenticator) is introducedand safety is improved further. The authentic method of Kerberos is shown in Drawing 8.
[0038]As for the authentic method of Kerberosall exchanges between each server and user WS are encipheredFurthermoresince it is generated by the enciphering key with the random number each timethere is no necessity that a point strong against tapping and the purpose server manage the user ID and the password of user eachand it is pointed out as a strong point that only the Kerberos server should know them etc.but. - Reuse the intercepted certification information as it isand possible (replay attack)if it is in fixed time.
[0039]- The Kerberos products in which DES as a cryptographic algorithm was mounted may be unable to be used in Japan for the export restrictions of the code products in the U.S.
- Since an authentication server carries out central control of each user's certification information and enciphering keyif a holder in bad faith succeeds in invasion to this authentication serverthat management symmetrical domain will be destroyed totally.
- Demeritslike Kerberos correspondence is required for all the machine and applicationand the time and effort of introduction is large are also pointed out.
(6) A zero knowledge dialog proof method this gentleman type is a method of which a partner is convincedwithout showing it having been proposed by Goldwasser of MITMicaliand Rackoff of University of Torontoand having a certain information in 1985 against the contents.
For exampleit is an example of use that it can prove against knowing the true passwordwithout showing a password etc.
The phi owt SHAMIA method will be proposed by Fiat and Shamir in 1986and it is a U.S.

Pat. No. 4748668 item (JP63-101987A).
[0040]The sequence by a zero knowledge dialog proof method in case the client A (testifier) transmits the secret information Tincluding password etc.to the server B (verification person) is shown in Drawing 9. HereA gets to know $Z=T^2 \bmod n$ thoroughlyand B assumes that only Z and n are known. Heren is a composite number of the big prime numbers p and q. In this caseif B cannot factorize n into prime factorit is very difficult to obtain T.
[0041]** of the following - ** are repeated k times (reason of a dialog)and the justification of A is verified.
** A chooses the random number Rcalculates $X=R^2 \bmod n$and sends X to B.
** B chooses b** {01} at random in alternativeand sends b to A.
** A is Y (in the case of b= 0Y is R.).
the case of b= 1 -- TR modn -- it is -- it sends to B.

[0042]** B inspectsand if these are realizedit will consider as the inspection O.K. whether in the case of $X= Y^2 \bmod n$ b=0the case of $ZX=Y^2 \bmod n$ b=1 is materialized. It is because client A' of the bad faith which dividing in the case of b= 0 and b= 1 was set to Aand was cleared up by ** and ** here can pass an inspection as follows even if it does not know the value of T. That isif it is always b= 1A will define Y' suitable as a value of Y by **will calculate $X=(Y)^{2}/Z \bmod n$and will send this X to B. Nextif the value of Y=Y' is sent by **naturally the inspection of ** will pass. Since X and Y which fill an inspection type with this method after expecting the value of b are calculablethe spoofing probability per time is 1/2 repeatedly. Thereforeif this procedure is repeated k timesspoofing probability will be made to 2^{-k}.
[0043]Since the strong point of this method does not need to teach the secret certification information T a priori to the server Bit is being unable to become the client A completelyeven if it is a just administrator of the server B.
The point that a dialog sequence is redundantand an authentication process are complicatedand the point that performance and authentication precision serve as a relation of trade-off etc. are demerit.

The <living body feature use> The conventional security which used the living body feature (personal attribute) next is explained.
[0044]This technique is a technique which uses the physical and aggressive feature of the person himself/herself as certification informationand checks a terminal user's justification. There is the following as a physical and aggressive feature.
- A bodily features fingerprinta voice spectrumthe pattern of a facea noteretina patternsthe form and the aggressive feature signature of an eara writing patternand a keystroke this gentleman typeSince the only personal attribute which it cannot have only in the person himself/herself is used as certification informationthe person himself/herself when attestation is successful -- although discrimination precision is highhe is the just person himself/herself -- being also alike -- recognition accuracy having the room for the technical improvement instead of 100%and in off-line attestation (local authentication)such as attestation of the user by a terminalalthough it is very effective that it is not involved but attestation goes wrong etc.In the attestation (remote attestation) which straddled the networkthere is a faultlike reuse (replay attack

etc.)i.e.spoofingbecomes possible about certification information by tapping.
[0045]The security by possessions use is explained.
<Possessions use> A certain specific object holds certification informationand attests softwarehardwareetc. which are interlocked with human being holding the objecthuman being attested by the objector its objectand operate as a just entity by verifying the certification information in the side to attest.
[0046]There is the following as an example of possessions.
- A keya tokena batchan electronic keya magnetic cardan IC card and a noncontact card (said to be the developed type of IC cardssuch as an optical type and an electromagnetic wave type)
For examplehuman being who possesses the key for canceling the lock of a terminala tokenand an electronic key is attested as a just user of the terminal.
[0047]Howeverin order to prevent the improper use by loss and the theft of these possessionsin attestation through a network. It is used combining the technique of "knowledge use"such as possessions performing user discernment first like a magnetic cardand also checking a user's justification by verification of the password by servers (host computer of an access pointetc.)in many cases.
[0048]In an IC cardthis develops furtherthe IC card itself verifies first human being who is going to use the IC card by a passwordand it goes into authentication operation with the server which passed the network only after this was successful. IC card (namelyentitiessuch as human being verified by IC card) authenticating processing by a server is performed using the technique of "knowledge use" and "code use."
[0049]If this technique holds possessions strictlyspoofingby a third party has a difficult pointandgenerally the IC card usually has tamper-proof nature (Tamper Free).
It has composition which cannot write the information in a memory from the exterior. Thereforeby incorporating the point that the information depending on individualssuch as an encryption key and a passwordcan be stored and managed comparatively safelyand the security processing function itselfin an IC cardWhile the point etc. whose still safer authentication communication becomes possible are the strong pointsin the authentication system by possessions use. The point which needs input/output devices for exclusive use between the terminals used as the possessions and client when the mostSince the authentication sequence itself is using the technique of "knowledge use" and "code use" after all in the case of the authenticating processing which passed the network by magnetic cardan IC cardetc.although it is naturalthe point that demerit peculiar to them will also accompany etc. are pointed out as demerit.
[0050]
[Problem(s) to be Solved by the Invention]As mentioned abovewhile the various conventional entity authentic methods have the strong pointthey also have demerit. By the wayalthough the direct threat which entity attestation assumes is "spoofing" by illegal acquisitionsuch as a passwordWhen this "spoofing" is once successful and it is invaded into it by the systemit will be exposed to the threat of various malfeasancessuch as an alteration of dataand generation of file destruction and incorrect data. Such a threat may be caused by internal crimessuch as what [not only] is depended on unlawful access from the outside but a system administrator.
[0051]Thereforefor the system of the side accessedthe entity attestation which checks what the substance to access is can be said to be the defense network of the front line to

the threat on securityand the importance becomes large according to the degree of secrecy of a system. If the intensity to "spoofing" of the entity authentic method described here until now is summarized to the inaccurate entity of the exterior and an insideit will become as it is shown in Drawing 10.
[0052]Any method of the above is practical enough depending on the environment of a systemand compositionalthough there is a fault. Howeveras shown in Drawing 10it is most which cannot be defended to the threat by the internal crime of the bad faith of the human being well versed in systemssuch as a system administratorand even if it is a method which can be defended even ifthere is a faultlike authenticating processing becomes complicated.
[0053]As stated aboveentity attestation is a defense function of the front line to various threats on securitybut. In the Internet agefrom extensive [of the application field]and a viewpoint of interconnectivityintroduction is easystructure is easyand to be a sufficiently effective method is desired to a threat. Thenit is as follows when the matter required of a new authentic method is summarized based on the examination to the strong point of various above-mentioned authentic methodsand demerit.
(1) The certification information stolen by tapping etc. does not reuse by a third party.
[0054]For examplealthough one-time password methods (S/Key etc.) are filling this businessif the authentication token method with a digital signature is in the allowed time of that time stampit will be able to reuse a tapping token.
(2) Certification information should be saved at an authentication server. If it puts in another waythe authentication server does not need to keep the certification information of user eachand should just have a function in which it is just discriminable whether the certification information at the time of login is just. By thiseven if a holder in bad faith is able to invade into an authentication servercertification information of user each cannot be acquired.
(3) An authentication sequence be easy as much as possible.
[0055]Therebyload to a system is made into the minimum and stability of operation is obtained. Thereforea dialog sequence like a challenge response method or a zero knowledge dialog proof method is not used.
(4) Certification information should differ each time andmoreoverthe information should exist infinitely. This satisfying the business of (1)when a password is exhausted like the existing one-time password methods (S/Key etc.)the fixed work of re-registering initial information into a server again becomes unnecessary.
(5) Don't need special external measurement apparatus like the living body feature use.
[0056]Since special apparatus spoils the compatibility through the Internet and it leads to the jump of introduction costsuch an external instrument is not used. In this waythis invention aims to let reuse by third partiessuch as certification information stolen even if certification information etc. were stolenprovide a difficult authentication methodan authentication devicean authentication serveretc. using the authentication method by an easy procedure.
[0057]
[Means for Solving the Problem]This invention is characterized by a way an authentication person attests an authentication demand person with a public-key crypto system comprising the following to a demand of attestation from an authentication demand personin order to attain an aforementioned problem.

A preservation process of saving the 1st examination report for an authentication person to inspect an authentication demand person's certification information beforehand.
An authentication demand sending-out process that said authentication demand person sends an authentication demand to said authentication person.
Said authentication person is a **** certification information demand process by sending a certification information demand to said authentication person to an authentication demand sent by said authentication demand person.
In order for said authentication demand person to answer said certification information demand and to generate certification informationwhile said authentication demand person sends the 1st certification information that enciphered and generated the 1st species information that self holds using said authentication demand person's secret key to said authentication personA certification information sending-out process of changing said 1st generated certification information to said 1st species information currently held as the 2nd species information for a next authentication demandand saving itand said authentication personBy decrypting said 1st certification information sent by said authentication demand person by said authentication demand person's public keyGenerate the 2nd examination report and a comparison process in comparison with forward [said]with said 1st saved examination report and said authentication person this 2nd examination reportAn updating process of notifying said authentication demand person of permitting said authentication demand when said 2nd examination report is in agreement with said 1st examination reportand replacing with said 1st examination report and saving said 2nd examination report.

[0058]According to this authentication methodan authentication demand person sends to an authentication person by making into certification information what enciphered species information (certification information used last time at the time of login) for generating certification information with an own secret keyAn authentication person decrypts certification information received from an authentication demand person by an authentication demand person's public keyand authenticating processing is attained by inspecting whether they are the same as compared with an examination report (certification information used last time at the time of login) of certification information which is an attestation side and had been saved.
[0059]Thereforesince he cannot generate certification information even if the 3rd person can know an examination report saved by the species information [which is saved by the authentication demand person side]and authentication person sideas long as an authentication demand person is keeping an own secret key strictlyspoofingby the 3rd person is impossible. If they are the same as compared with a certification information examination report (certification information used at the time of the last login) which compounded certification information received from an authentication demand person by an authentication demand person's public key in the authentication person sideand had been saved by the authentication person sideSince the certification information is immediately saved as a next certification information examination reporta time lag it becomes possible to intercept certification information which the 3rd person is transmittingto reuse it as it isand to impersonate an authentication demand person is zero substantiallyand impossible.
[0060]In order to apply this authentication methoda certification information file server

which saves certification information for giving attestation to an authentication demand from two or more authentication demand persons concerning this inventionA means to memorize an examination report for inspecting an authentication demand person's certification information for every authentication demand personA means to send a certification information request message to the authentication person if an authentication demand from arbitrary authentication demand persons is receivedCertification information sent by the authentication demand person is decrypted by the authentication demand person's public keyWhen an examination report is newly generated and a means [forward / said /with a saved examination report / examination report / this / that was newly generated] and said newly generated examination report are in agreement with said saved examination reportpermit said authentication demandand. A means to replace with said saved examination report and to save said newly generated examination report is provided.

[0061]An authentication device which gives attestation to an authentication demand from an authentication demand person is provided with the following with support of an external authentication server of suitable this invention for the above-mentioned authentication method.

A memory measure which memorizes species information for generating certification information which attests said authentication demand person.

A transmission and reception means which an authentication demand message is sent to said authentication serverand receives a certification information request message from said authentication server which answers this authentication demand message.

An encoding means which generates certification information to a certification information request message from an authentication server by enciphering said species information memorized to said memory measure using a secret key.

An attestation delivery means which generated certification information is sent to said authentication serverand changes to said species information memorized in said memory measureand memorizes this generated certification information.

[0062]This invention is characterized by that a terminal unit usable in an unspecified user comprises the following again especially.

To an authentication demand by a specific authentication demand personan authentication terminal device which gives attestation to an authentication demand through a storage from an authentication demand person supported by an external authentication server of high this invention of security is a main part.

Have an interfacing means for receiving a storage which memorizes a program which generates certification information using said secret key from species information for generating certification information which attests an authentication demand persona secret key about the authentication demand personand said species informationand said main partA reception means which receives an authentication demand from said authentication demand person.

A request means which answer this authentication demandand an authentication demand message is sent to said authentication serverand receives a certification information request message from said authentication server which answers this authentication demand.

Answer a certification information request message and via said interfacing meansAre a

commanding means which performs a program in said storageand said program is receivedreturn certification information which was made to generate this authentication demand person's certification information using said secret keyand was generated from said species information to said main part via said interfacing means -- it closing and. A commanding means which makes said species information in said storage update by this generated certification informationand a means to send returned certification information to said authentication server.

[0063]It can apply also to a storage which memorizes a program used for a device which the authentication demand person side uses when applying the above-mentioned authentication methodand this invention is **. In order that this this invention may generate certification information with which said authentication program attests said authentication demand personit is characterized by a storage which memorizes an authentication program which gives attestation to an authentication demand from an authentication demand person with support of an external authentication server comprising the following.
The 1st program code that makes a predetermined memory measure memorize species information.
The 2nd program code that sends an authentication demand message to said authentication server.
The 3rd program code that receives an authentication demand message from said authentication server.
Send the 4th program code that generates certification information using a secret key from said species information memorized to said memory measureand generated certification information to said authentication server to a certification information request messageand. The 5th program code that changes to said old species information and memorizes this generated certification information as new species information.

[0064]When depending on one suitable mode of this invention and a notice of a purport which permits an authentication demand is receivedspecies information is updatedand when a notice is not receivedit does not update. It is for collateralizing the identity of species information by the side of an authentication demand personand an examination report by the side of an authentication person. If it depends on one suitable mode of this inventionsaid authentication demand person's identification information will be used as an initial value of said 1st species information.
[0065]If it depends on one suitable mode of this inventioncertification information will be sent to an authentication server with an authentication demand person's public key certification. Acquisition of a public key of an authentication demand person in the authentication person side becomes easy and certain. If it depends on one suitable mode of this inventionsaid memory measure will memorize a public key certification for every authentication demand person with an examination report. It becomes unnecessary to send a public key certification at the time of next login.
[0066]If it depends on one suitable mode of this inventionan authentication demand will be refused when examination reports are not in agreement in an authentication person. If it depends on one suitable mode of this inventionit is enciphered that only a genuine owner can decrypt said authentication demand person's secret key. A secret key is

protected.
[0067]Said storage will be an IC card if it depends on one suitable mode of this invention. If it depends on one suitable mode of this inventionsaid storage memorizes a password further and compares further a password entered by said authentication demand person with a password memorized by said storageand only when in agreementsaid storage will return certification information to said main part.
[0068]If it depends on one suitable mode of this inventionconversion to certification information from species information using a secret key is performed only in a storageand said secret key will not be sent to said main part sideand will be made. An important secret key does not come out of a storage.
[0069]
[Embodiment of the Invention]The suitable embodiment thru/or example of this invention is described referring to an accompanying drawing below. In this network that shows the composition of the network with which the method which Drawing 11 requires for this invention is appliedtwo or more client 200300 -- is connected by the Internet. The authentication server 100 is also connected to this network.
[0070]When the client 200 communicates with the client 300the client 200 serves as an authentication demand personand the client 300 serves as an authentication person. According to this embodimentan authentication person is called a server. The authentication server 100 has an accessible database from two or more clientsattests in response to the authentication demand from these clientsand calls it an authentication server. Refer to Drawing 12. That iswhen a client and a client communicateone side acts as a server.
[0071]The authentication method of this embodiment is not premised essential on existence of a certificate authority (CA). Since the intervention of a certificate authority (CA) is not needed and it is carried out directlytransmission and reception of the data between clients may be performed via the authentication servers 100 (for exampleCA etc.). It is a computer (or system) by which the authentication person and authentication demand person also operates through the act of not the person itself but an operatoror a user.
[0072]Drawing 13 shows the example of the authentication algorithm which applied this invention in the network (Drawing 11) which consists of simplified composition with authentication server Y as the client X and authentication person as an authentication demand person. In the example of Drawing 13a public-key-encryption algorithm is used as a premise. The client X presupposes the server Y again that public key K_P corresponding to secret key K_S of the client for own secret key K_S and certificate CK_p of the public key are held. As for $S_e$the encryption function of a public-key-encryption algorithm and S_d mean the decryption function of a public-key-encryption algorithm.
[0073]In this systemas shown in Drawing 13a client side has the certification information generation kind data file 204and the server side has the client authentication information inspection data file 105. The certification information generation kind data file 204 is a file which memorizes the data used as the kind for generating certification information. Herein this systemcertification informationmeans the information which an authentication demand person sends to an authentication personin order that an authentication demand person may make demands on an authentication person for attestationand in a client sideit is generated from seed data. If this I/O information carries

out **** collation by the inspection of that client that a server has in the server side and collation can be takenit will consider that that client is a genuine authentication demand person.
[0074]Drawing 14 has the composition of the certification information inspection data file which the server Y has. namelythe server Y has "certification information inspection information D"and "public key K_P" and "public key certification CK_p for every client. In the example of Drawing 14the server Y has inspection information D_X and public key K_{PX} about the client Xand has inspection information D_W and public key K_{PW} about the client W.
[0075]in order that Drawing 15 may realize attestation of this embodiment -- the client X and the server Y -- the procedure which is boiledrespectively and can be setand the procedure of connection performed among these are shown. The case where it is going to receive the attestation at the time of the client X logging in the procedure of this embodiment to a server according to Drawings 13 and 15 is explained.
<Registration of initial information> In this embodimentit is required for a client to set up initial seed data D_{S0} in advance of loginand to register initial-inspection data D_{s0} in first stage in the server Y. Once what is necessary is to perform these registration only once first and it carries outregistering after that is unnecessary.
[0076]In a client sidesince the client itself performs this registering operation and it generally follows setting out of the access permission of a clientetc. on the server sideit is preferred that a system administrator with suitable authority carries out. An E-mail addressa user identifieretc. of a random number or a client of initial seed data D_{S0} are [anything] good. If even secret key K_s is maintained at the secreta client will be notified that it was registered after the registration which does not have to make initial seed data D_{S0} secret in particular.
[0077]Seed data D is used in a client for generation of certification information so that it may mention later. And once the authentication demand using the certification information is acceptedthe generated certification information will be memorized as seed data for the certification information generation for the authentication demand for the next login. In the server sideif the received certification information is compared with inspection information D saved beforehand and collation is obtainedthe received certification information is saved as inspection information for login of the next from the client. Thereforesince the seed data memorized by the certification information generation kind data file 204 and the inspection information memorized by the inspection data file 105 by the side of a server are in agreement as a valueit expresses with this system as D_{n-1} for convenience in Drawing 13. Seed data and inspection information were generally expressed as D_{n-1} because those data was generated in the last login.
[0078]In the example of Drawing 13the initial seed data of the client X is registered as D_{S0}. The Challenge Handshake Authentication Protocol of this embodiment generates certification information from this initial seed data $D_{S0}$when the attestation which the client X begins is permitted. Whenever the session for attestation is completedseed data D_{n-1} saved until now is enciphered by secret key K_S of the client Xand the big feature is at the point of saving it as seed data D_n for a next attestation session. The last seed data D_{n-1} may be saved for maintenance of a historyalthough not used in login on and after next time.
[0079]Hereafteraccording to Drawings 13 and 15the procedure of this embodiment is

explained in order of.
- According to a step ** book embodimentattestation attests whether the client which tries to log in is a genuine client.Thereforelogin in a server is performed in advance of attestation. Login by this embodiment is performed by sending user identifiers (User-id etc.) to the server Y. The form of a cryptogram with a plaintext may be sufficient as this login message.
[0080]- The server Y which received the step ** login message sends a certification information request message to the client X.
- Step ** The client X which received this certification information request message enciphers seed data D which self saves by own secret key K_S as certification information which should be returned to a serverand sends it to the server Y.
[0081]By beginning the example of Drawing 13 after initial registrationsince it is the start of an attestation sessionthing D_1 which seed data is D_{S0}therefore enciphered data D_{S0} by secret key K_S of the client X is sent to the server Y.
- The step ** server Y will be decrypted by public key K_P of the already obtained client Xif certification information D_1 is received from the client X. As mentioned abovecertification information D_n of this embodiment is enciphered according to the public-key-encryption-ized algorithm. Namelyif enciphered by secret key K_S of the client Xcertification information D_1 which should express the client X genuine seed data D_{S0} of the client XWhat decrypted the certification information D_1 by public key K_P must be in agreement with seed data D_{S0} before being enciphered by secret key K_S of the client Xif a public-key-encryption-ized algorithm is followed.
[0082]- Step **then the server Y carry out comparative collation of information D_{S0} decrypted and obtained and the inspection information D_{S0} of the client X read from the file 105.
- A step ** server returns a collated result to a client.
[0083]As mentioned abovewhen collation is in agreementsince the client X which required attestation means being a genuine clientit returns the message of a purport which permits login. It prepares for the login request from the next client Xand certification information D_1 as which the place received from the client X is enciphered is saved in the file 105. Renewal of this certification information in the server Y (overwriting) is performed only when the comparison result in step ** is in agreement. Encrypted authentication information D_1 written in in the file 105 is memorized as inspection information for next login within the file 105.
[0084]- the client which received the authenticating processing result from a step S** server -- the authenticating processing result -- permission -- or judge whether it is refusal.
- When step S** attestation is permittedmemorize certification information D_1 currently sent to the server side to the file 204 as seed data D_1 at the time of next login.
[0085]Since certification information D_1 cannot be used as seed data D_1 at the time of next login when attestation is refused (it contains also when a processing result does not come on the contrary within predetermined time)it cancels. If it puts in another wayin retrying logina client generates again certification information $D_{1\text{from seed data }DS0}$. It is the procedure for the attestation to a login request when the above begins and login is performed.
[0086]When login is performed next timestep ** - ** are repeated. That isas shown in Drawing 13the client X is enciphered and generated by that secret key K_S by making

saved seed data D_1 into certification information to the 2nd certification information demand from the server Yand sends this enciphered certification information D_2 to the server Y. The server Y decrypts sent certification information D_2 by public key $K_P$generates inspection information $D_1$and compares with inspection information D_1 which stored this inspection information D_1. If coincidence of comparison can be takenit is the same as the time of the first login at the point of permitting login.

[0087]Since this method is restricted at once and can generate effective certification information infinitelyit is made to call this an "infinite onetime authentic method" henceforth. The advantage which should be emphasized [the conventional system of this infinite onetime authentic method / especially] is as follows.

(1) Only the just authentication demand person can generate the certification information generated next time at the time of login using the secret key which he holdsand even the certification information administrator of not only an external third party tapping person but a server cannot know certification information for the next time. It is possible to prevent by thisthe malfeasance by "spoofing"i.e.the internal crimeto the user by an internal bad faith person by the side of a server.

[0088]Namelythe thing as which the authentication demand person enciphered generation seed data (certification information used last time at the time of login) with the own secret keyIt sends to an authentication person as certification informationand an authentication person grants a permission to an authentication demandonly when in agreement as compared with the inspection information which decrypted the certification information received from the authentication demand person by the authentication demand person's public keyand was saved by the authentication person side. Thereforeas long as the own secret key is being kept strictlyeven if certification information generation certification informationinspection informationor seed data (or wholly) will be known by the 3rd personspoofing of the client concerned by the 3rd person is impossible.

[0089]In an authentication personinspection information is compared in one authentication demand treatment processnot being in agreement -- or promptlysince inspection information is updated if it does not escape from the treatment process and coincidence can be taken until it is checked that it has been in agreementThe time lag to renewal of inspection information is zero substantiallytherefore the postponement time of the 3rd person intercepting the certification information under transmissionreusing it as it isand impersonating an authentication demand person is zero substantially.

(2) Registration of certification information can be managed once with a limitationand if it registersthe client can once generate the high certification information of security infinitely. Howeverwhen the pear of a secret key and a public key is changedit is necessary to register with a server again.

(3) The authenticating processing between client servers does not have a dialog sequencebut it is only transmitting one message (certification information) at the time of login. Thereforethe program needed by the server side and a client side will become very easy.

(4) A time interval after sending certification information to the server side by a client side until it updates the certification information to the following certification information (namely$D_{[\ \text{from}\ Dn\ ]\ n+1}$ updating) is equal to zero. Thereforeeven if certification information is intercepted during communicationthere will be no time crevice in which a tapping person can reuse it.

[0090]On the other handin a method which uses a time stamp for a part of certification information by the existing method. Since fixed time tolerance level is provided by the server sideif the reuse of the certification information is carried out immediately [after-tapping] within the tolerance level timethe timing (replay attack) which can log in to a server may existbut this is impossible in this method.
(5) Even if internal authorized personnelsuch as a server managerused inspection information D_n by stealth for the server side and it tried false attestationD_n which these persons usedthe public key of an authentication demand person genuine in an authentication process -- **** -- since it is compared with D_{n-1}-izing [**] and generatedattestation is not successful. That iseven if it is internal authorized personnel who can know the certification information of a servera genuine authentication demand person cannot be become completely.
[0091]
[Example]The example which materialized the above-mentioned infinite onetime authentic method is described below. Drawing 16 shows the server side composition for this example. WINDOWSMAC OSUNIXor NETWARE is used for this server as OS101for example. The communications protocol with the network 102 uses TCP/IPOSIand NETWARE.
[0092]The inspection data file 105 has the composition of the file explained in relation to Drawing 14andspecificallymemorizes the identifier information X on a clientand inspection information D_{n-1} and public key certification CK_{px}. Public key certification CK_{px} includes a version numbera serial numberan issue station namethe term of validity of a certificatea user-identification childa public keypertinent informationetc. The public key file 107 saves public key K_{pc} of certifying authority CA. It is used for this public key K_{pc} inspecting the digital signature given to the public key certification of the client X.
[0093]By inspecting public key certification CK_{px} of the client Xthe decoding processing program 106 obtains K_{Px}decrypts certification information D_n (enciphered by secret key K_S of the client) which received by public key $K_{Px}$and generates inspection information D_{n-1}. Drawing 17 shows the composition of a client side. WINDOWSMAC OSUNIXor NETWARE is used for this client system as OS201for example. A communications protocol uses TCP/IPOSIand NETWARE. In this caseit is necessary to coincide the communications protocol of a client side with the communications protocol by the side of a server. Howeverit is not necessary to coincide OS of a client side with OS by the side of a server. The secret key file 206 is a file which saves secret key K_S of the client X concerned. As for this secret key $K_S$being enciphered by the predetermined enciphering procedure is preferred.
[0094]Encryption to certification information $D_{[\text{ from encryption of secret key KS and decryptionand certification information seed data Dn-1 using secret key KS further] n}}$ is performed by the encryption processing program 207 with the help of the authenticating processing program 202. The certification information generation kind data file 204 memorizes the seed data for certification information generation of the client X.
[0095]The authenticating processing program 104 by the side of a server performs the control procedure on the right-hand side of Drawing 15and the authenticating processing program 202 of a client side performs the control procedure on the left-hand side of [the] a figure. The feature of the example system of Drawing 17 has the feature in the point of enciphering and keeping secret key K_S on the local disk of a client side system.

As for the client system of Drawing 17the infinite onetime authentic method concerning the embodiment which this showed in Drawing 12 etc. attains the controlling function by encryption of secret key $K_S$sake [keep / own secret key K_S / the client X / strictly / premised].

[0096]It is [treatment process / 207 / encryption] usable in various things. For examplealthough the technique of requiring a password of the user who uses ** 17th figure system is also simpleit is preferred to encipher and keep K_S by using as a key the passphrase which the client X gets to know using a suitable common key encryption system like DES. As a resultit is lost that K_S becomes known to a third partyand the parenchyma top of becoming the client X and clearing up becomes impossible. Moreover it can keep K_S secretly only by not needing extra hardware but installing code softwareeffectslike external-interface apparatus is unnecessary and there is can be acquired.

[0097]Operativityextendibilityand variability improve by leaps and bounds by forming the cipher-processing program 207 into a plug-in program module especially. The gestalt which sends public key K_p of a client to a server can consider various gestalten. The server side is premised on obtaining the public key certification of the client X from a client for every login in the example of Drawing 16. That isfor examplea client sends public key certification CKp_x of the client X with the certification information sent to a server.

[0098]The authenticating processing program 104 by the side of a server will return a certification information request message to a clientif the login message of the client X is receivedand. The digital signature of proof office CA given to the user's X public key certification which came to hand is inspected using public key K_{pc} (saved in the file 107) of proof office CA. If an inspection is checkedit will be checked that the public key certification is a just public key certification of the client X. Public key certification CK_{px} of the client X is saved at the file 105. The program 106 accesses the data file 105 and takes out public key K_{px} of the client X in public key certification CK_{PX}.

[0099]<Modification> This invention can change variously in the range which does not deviate from the meaning.

The 1st modification: For examplein the example of 16 figurethe public key certification of a client is made to be transmitted to the server side from the client for every login. In this methodsince it is not necessary to make the public key of a client secretit is not necessary to send the public key certification of the client X for every login each time.

[0100]Thenif login from the client X is in the login process of the program by the side of a serverit will propose adding the procedure of inspecting whether the public key certification CK_{px} of X already being kept in the file 1O5. In that casebefore it sends a certification information request message to the clientit may be made for the server side to send a public key certification request messagewhen there is login from the client into which the public key certification is not registered.

[0101]The 2nd modification: The above-mentioned example has inconvenient [that the client terminal used for login is limited to the terminal which is keeping K_S]. Thensecret key K_S is kept not on a client terminal but on an IC cardand it proposes that the client X always walks around with the card. The composition of the system of a client side for that is shown in Drawing 18. The system of Drawing 18 is at the password file 301 which memorizes a user's password to IC card 300the file 302 which memorizes a public key

certificationthe file 304 which memorizes secret key $K_S$and the point of having especially the cipher-processing program 304.
[0102]When the system shown in Drawing 18 is considered as client side compositionthe server side composition can use ** 16th figure composition. Drawing 19 illustrates the coordinated movements of the authenticating processing program 308 (client host side) of the client side of Drawing 18and the cipher-processing program 303 (client card side).
[0103]Firstif there is login (for examplean IC card is made to read into an unillustrated card reader) by a userthe cipher-processing program 303 will send the request message (request message of a password) of certification information to a client via the authenticating processing program 308 of a terminal. If a user is a regular userthe right password will be entered from the keyboard etc. which is not illustrated [of a terminal]. If the password is enteredthe program 308 will send the entered password to the cipher-processing program 303 via an interface. The cipher-processing program 303 compares the received password with the password memorized in the file 307.
[0104]Since a message to that effect is returned to the authenticating processing program 308 if not in agreementthe authenticating processing program 308 refuses the login concerned. If coincidence is obtainedthe cipher-processing program by the side of a card will report that the thing which publish the utilization permission of an IC card to a client and for which an authentication demand is both performed to an authentication server was permitted.
[0105]Nexta client performs the authentication demand to an authentication server. Future procedures are as having explained in Drawing 13. In this casein a client sideit is important that all encryption by secret key K_s for generating certification information from seed data D_{n-1} is performed by the cipher-processing program 303 in IC card 300. That isany information about secret key K_s does not get across to the host sideand certification information D_n is transmitted. It is because certification information D_n cannot decode it even if it is seen by the 3rd person as mentioned above.
[0106]It is not preferred that the secret key file 304 is opened (fear of disclosure or an alteration) to the authenticating processing program 308 in the client side system of Drawing 18. It is because it is not preferred that many unspecified users may use the host system of a clientand secret key K_s is put to a host system in a raw form. Thenit is preferred to encipher secret key K_s in the file 304 according to cryptographic algorithmssuch as DESwith the password in the password file 307. Since it is enciphered by DES even if for examplethe authenticating processing program in a host is altered and secret key K_s is read from the file 304 if secret key K_s is encipheredthere are very few possibilities that it will be decoded.
[0107]Since K_S is saved at an IC card according to this modificationhe is unable for a third party to become the client X person himself/herselfand to clear up using a client terminal. as long as it puts in another waythe system of a client side may be a general-purpose personal computer -- this personal computer -- a client -- it enables the person of an except to use it the X person himself/herself. If it is a terminal in which an IC card and an interface are possibleit will become usable as the client side main frame at any terminals. Thereforea remote login etc. become possible from outside the companyfor example with a personal digital assistant. Since the IC card is considering it as the method which attests the client X (user) by a password etc. in advance of login processing executioneven if it loses an IC cardit is difficult for the third acquisitor to

become the client X and to clear up.
[0108]The 3rd modification: In additionalthough the server itself saves the public key of a client beforehand or it was premised on the gestalt that a server orders from a clientin the above-mentioned embodiment and the exampleand also the modificationAs mentioned abovehis public key once sent from the client is kept by the server sideand the kept public key may be diverted with a certificate in future login. It is because a public key may be known by others. Howeveras for a certificateit is preferred that I have a public key certification resent with the technique of having mentioned above to login after shelf-life progress since the shelf-life was set up (thereforealso in case of public key).
[0109]The 4th modification: In the above-mentioned embodiment and an exampleand also the modificationalthough premised on existence of a networkthis invention does not make a network requirements again. Aboutif attestation is requiredthis invention is applicable also between a host and an input/output devicefor example.
The 5th modification: Although the problem of the attestation at the time of an exchange of the data which it was probably radio although it was probably a cable (but)and passed the communication line was dealt with in the above-mentioned embodimentfor examplethis invention can also be applied to the closing mechanism of the door using a card. That islock climate acts as an authentication server in this case.
[0110]
[Effect of the Invention]As explained aboveaccording to this inventionthe advanced authentication method by an easy procedurean authentication devicean authentication serveretc. can be provided. That issince there will almost be no time for the 3rd person to reuse it as it is even if it is strong to a repeat attack and the certification information under transmission is stolensince an examination report and seed data are changed each timesecurity is maintained. Even if species informationcertification informationor inspection information is stolenas long as management of the secret key of a client is performedit is very difficult for a third party to reuse the stolen certification information.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The figure explaining the classification of attestation.
[Drawing 2]The figure explaining the outline of the conventional challenge response method.
[Drawing 3]The figure explaining the common model of a public-key crypto system.
[Drawing 4]The figure explaining the conventional attestation child checking method.
[Drawing 5]The figure explaining the conventional authentication token method with digital proof.
[Drawing 6]The figure explaining the conventional SSH method.
[Drawing 7]The figure explaining the outline of the conventional RPC attestation.
[Drawing 8]The figure explaining the outline of a Kerberos authentication method.
[Drawing 9]The figure explaining the outline of a zero knowledge dialog proof method.
[Drawing 10]The figure in which the demerit of the various conventional security systems was summarized.

[Drawing 11]The figure showing theoretically the composition of the authentication system concerning the embodiment of this invention.
[Drawing 12]The figure showing theoretically the composition of the authentication system concerning the embodiment of this invention.
[Drawing 13]The flow chart explaining the example of an operation result of the authentication procedure by the embodiment of this invention.
[Drawing 14]The flow chart explaining the authentication procedure by the embodiment of this invention.
[Drawing 15]The figure explaining the composition of the certification information file memorized by the authentication server concerning the embodiment of this invention.
[Drawing 16]The figure showing the system configuration by the side of the server of the example of this invention.
[Drawing 17]The figure showing the system configuration of the client side of the example of this invention.
[Drawing 18]The figure showing the system configuration of the client side concerning a modification.
[Drawing 19]The flow chart explaining the procedure of the client side concerning a modification.